REMARKS

Claims 9-13 and 18-28 are currently pending in the subject application, and are presently under consideration. Claims 9-13 and 18-28 are rejected. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 9-13 and 18-28 Under 35 U.S.C. §102(b)

Claims 9-13 and 18-28 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,757,920 to Misra, et al. ("Misra"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

It is respectfully submitted that the rejection of claims 13, 25 and 27 as being anticipated by Misra was made in error. It appears that claims 13, 25 and 27 were mistakenly rejected under an anticipation rejection and an obviousness rejection, wherein there are specific arguments set forth only for the obviousness rejection of claims 13, 25 and 27. Accordingly, only the obviousness rejection will be addressed in the present response.

Claim 9 recites encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with the token identification in the database to form a download packet, downloading the download packet to the token, and activating the certificates/private keys in the download packet using a private key in the token.

Misra does not anticipate claim 9. In response to the arguments set forth in a previous response to an Office Action, the Examiner has cited sections of Misra that the Examiner contends disclose elements of claim 9 (See Office Action, Page 2). Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claim 9. Misra discloses that a digitally signed and sealed certificate is created by initially generating a hash of the contents within the signed and sealed certificate (See Misra, Col. 5, Line 65-Col. 6, Line 3). Misra also discloses that a one

way hash function is used to generate the hash of the contents of the digitally signed and sealed certificate (See Misra Col. 6, Lines 3-5). In contrast, claim 9 recites encrypting all certificates/private keys using a public key associated with a token identification in a database. As stated in Misra, the hash function is a one way function. By definition, a one way function cannot be decrypted. Conversely, the certificates/private keys encrypted with the public key recited in claim 9 can be decrypted with the public key's associated private key (the private key in the token). Thus, the hash function disclosed in Misra is a completely different type of encryption from the encrypting recited in claim 9. Therefore, the hash of the contents within the signed and sealed certificate does not correspond to the download packet recited in claim 9. Accordingly, the cited section of Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claim 9.

Misra also discloses that a user may request to download a logon certificate to a removable storage media, such as a floppy diskette, and when the user requests to download the logon certificate, the user is prompted to supply a password (See Misra, Col. 6, Lines 63-67). Misra also discloses that a one way hash function is used to hash the password, which is used to generate an encryption key, which is used to encrypt the logon certificate (See Misra, Col. 6, Line 67-Col 7, Line 3). Further still, Misra discloses that the password can be later used to generate an encryption key, which can be used to decrypt the logon certificate so that it can be retrieved from the remove storage media (See Misra, Col. 8, Lines 27-31). Thus, the password disclosed in Misra can act as a symmetric key, that is, a key can encrypt and decrypt the same data. Conversely, in the public and private key pairs recited in claim 9, when a data has been encrypted with the public key, that data can only be decrypted by a corresponding private key, and not the public key. Thus, the encrypted certificate on the removable storage media disclosed in Misra is not encrypted using public/private key encryption, but rather symmetric encryption. Therefore, the encrypted certificate disclosed in Misra does not correspond to the download packet recited in claim 8. Therefore, the cited section of Misra does not disclose encrypting all

certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claim 9.

Misra also discloses that logon certificates may be created though the use of asymmetric encryption (public/private key encryption) mechanisms (See Misra, Col. 5, Lines 21-29). Misra further discloses that each domain has a an associated public and private key pair (See Misra 31-33). In contrast, claim 9 recites encrypting all certificates/private key using a public key associated with a token identification. Nothing in Misra discloses that any removable media, which the Examiner alleges reads on a token (See Office Action, Page 3), has an associated public key. Thus, the asymmetric encryption does not correspond to the encryption of all certificates/private keys, as recited in claim 9. Thus, the cited section of Misra does not disclose encrypting all certificates/private keys of a plurality of certificates/private keys which have not been downloaded to a token using a public key associated with a token identification in a database to form a download packet, as recited in claim 9. In fact, nothing in Misra discloses this element of claim 9.

Additionally, Misra does not disclose activating certificates/private keys in a download packet using a private key in a token. As stated above, the logon certificate disclosed in Misra is encrypted using a symmetric key scheme. Nothing in Misra discloses the employment of a private key during the decryption of the logon certificate disclosed in Misra. Consequently, Misra does not disclose activating certificate/private keys in a download packet using a private key in a token. Therefore, Misra does not disclose each and every element of claim 9. Accordingly, Misra does not anticipate claim 9, and therefore, claim 9 should be patentable over the cited art.

Claims 10-12, and 23-24 depend either directly or indirectly from claim 9 and are patentable over the cited art for at least the same reasons as claim 9 and for the specific elements recited therein. Accordingly, claim 10-12 and 23-24 should be patentable over the cited art.

It is respectfully submitted that the Examiner did not respond to all arguments set forth by Applicant for the rejection of claim 23. Therefore, the arguments shall be reiterated to

prepare for appeal. Misra does not disclose activating certificates/private keys further comprising the entry of a passphrase, as recited in claim 23. As stated above, claim 23 depends from claim 9. Claim 9, from which claim 23 depends, recites activating the certificates/private keys in a download packet using a private key in a token. Thus, claim 23 recites (by virtue of its dependence from claim 9) activating certificates/private keys by using a private key in a token and entering a passphrase. It is respectfully submitted that in rejecting claim 23, the Office Action attempts to use the same aspect of Misra (a downloading password) that was used in the rejection of claim 9 for disclosing two separate elements recited in claim 23, namely, the private key and the entry of a passphrase. The United States Court of Appeals for the Federal Circuit ("Federal Circuit") has held that the doctrine of claim differentiation dictates that where claims use different terms, those differences are presumed to reflect a difference in the scope of the claims. *Forest Laboratories, Inc. v. Abbott Laboratories*, 239 F.3d 1305, 1310, 57 U.S.P.Q.2d 1794 (Fed. Cir. 2001). If both the private key and the passphrase were considered to be the same element, claim 23 would be superfluous.

As discussed above with respect to claim 1, in Misra, the password alone can be used to decrypt the logon certificate. There is no requirement in that any other entity (and particularly not a private key) is needed to decrypt the logon certificate disclosed in Misra. In the response to the arguments against the rejection of claim 23, it is respectfully submitted that the Examiner has not addressed the issue of claim differentiation. Thus, it is respectfully submitted that claim 23 is not given independent patentable weight. Accordingly, Misra does not disclose each and every element of claim 23.

Regarding claim 18, Misra does not anticipate claim 18 for substantially the same reasons as claim 9. As stated above with respect to claim 9, Misra does not disclose encrypting all certificates/private keys of a plurality of certificate/private keys which have not been downloaded to a token using a public key associated with the token identification in a database to form a download packet, downloading the download packet to the token and activating the certificates/private keys using a private key in the token, as recited in claim 18. Thus, Misra

does not disclose each and every element of claim 18. Accordingly, Misra does not anticipate claim 18, and therefore, claim 18 should be patentable over the cited art.

Claims 19-22, 26 and 28 depend either directly or indirectly from claim 18 and are patentable for at least the same reasons as claim 18 and for the specific elements recited therein. Thus, claims 19-22, 26 and 28 should be patentable over the cited art.

Additionally, claim 26 is not anticipated by Misra for substantially the same reasons as claim 23. That is, by virtue of the doctrine of claim differentiation, Misra does not disclose that activating occurs in response to a receipt of a passphrase, as recited in claim 26. Accordingly, Misra does not disclose each and every element of claim 26.

For the reasons described above, claims 9-13 and 18-28 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 13, 22, 25 and 27 Under 35 U.S.C. §103(a)

Claims 13, 22, 25 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Misra in view of U.S. Patent No. 6,192,131 B1 to Geer, Jr. et al. ("Geer"). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 13 and 25 depend from claim 9, while claims 22 and 27 depend from claim 18. The addition of Greer does not make up for the aforementioned deficiencies of Misra with respect to claim 9 and claim 18.

Additionally, regarding claims 13, 22, 25 and 27, it is respectfully submitted that there is no motivation to combine and modify the teachings of Misra and Greer in the manner suggested by the Office Action. Misra provides no teaching or suggestion to implement smart cards. Greer provides no teach or suggestion for the distribution of logon certificates. The Federal Circuit has held that it is insufficient to establish obviousness by showing that the separate elements existed in the prior art, absent some teaching or suggestion in the prior art to combine the elements. *Arkie Lures, Inc. v. Gene Larew Tackle, Inc.*, 119 F.3d 953, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997). It is respectfully submitted that without using improper hindsight, one skilled in the art

would not combine and modify the teachings of Misra and Greer in the manner suggested by the Office Action.

In response Applicant's arguments regarding the motivation to combine the teachings of Misra and Greer, the Examiner states that the motivation is the implementation in a smartcard (See Office Action, Page, 2). However, the Examiner has not set forth any reason (other than the present application) as to why one skilled in the art of smart cards would look to employ the teachings of Misra. In Misra, encrypted data is stored on a non-secure removable media (a floppy diskette). In contrast, a smart includes processing capabilities. Nothing in Misra teaches or suggests the removable storage media should include processing capabilities. Thus, there is no motivation to combine and modify the teachings of Misra and Greer in the manner suggested by the Office Action. Thus, Misra taken in view of Greer, does not make claims 13, 22, 25 and 27 obvious.

For the reasons described above, claims 13, 22, 25 and 27 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 4-17-06

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
1300 EAST NINTH STREET, SUITE 1700
CLEVELAND, OHIO 44114
Phone: (216) 621-2234
Fax: (216) 621-4072